Policy for Managing the Internal Information System (Whistleblowing Channel) in Spain

Policy Owner: Compliance

Effective Date: February 2026
Version: 1

1. Introduction and Purpose

This Policy establishes the fundamental principles that govern the operation of the Internal Information System (the "Internal Information System" or "System") of all companies that make up the ADM Group in Spain (hereinafter "ADM", "ADM Group" or the "Company").

ADM maintains an integrated Internal Information System to facilitate the detection, receipt, assessment, investigation, and resolution of reportable matters connected with ADM's activities, while ensuring confidentiality, independence, procedural fairness, and compliance with applicable data protection rules.

The Internal Information System aims at promoting compliance within the company with the provisions of the Principles of Responsible Business, the law and other applicable internal regulations by employees, managers, administrators of the ADM Group companies and other stakeholders. This system has the appropriate mechanisms to guarantee the confidentiality of communications and reports submitted through it, as well as the proper protection of the informant, the accused and other persons involved in the communication of any conduct that may fall within its scope. In this way, it reflects ADM's commitment to ensuring that the actions of the Company and its employees meet demanding standards of professionalism, integrity, and a sense of responsibility.

This policy sets governance principles, scope, safeguards, and minimum operating rules for ADM's Internal Information System.

2. Scope of Application

This Policy applies to ADM and to the entities forming part of its corporate group that operate in Spain or whose persons and activities are covered by the Internal Information System. It is binding for all persons who fall within the personal scope described in Section 5.

As permitted under Law 2/2023, all companies making up the ADM Group in Spain, considering their size, geographic scope, and the nature of their activities, share their Internal Information System and the resources allocated to the management and processing of Complaints, which will comply with the principles and criteria established in this Policy.

ADM Group entities may coordinate and share information strictly to the extent necessary for proper operation of the System and consistent with confidentiality, data protection, and the rights of involved persons.

Reports under this Policy must relate to:

- conduct, actions, omissions, or risks connected to ADM Group entities' activities, business relationships, and work-related/professional context; and
- matters within the material scope set out in Section 3.

3. Material scope of reportable matters

The behaviors that can be reported through the channels integrated into the Internal Information System are the following:

- Actions or omissions that may constitute violations of the European Union (hereby "EU") law in the following areas:
    - public procurement;
    - financial services, products and markets, and prevention of money laundering and terrorist financing;
    - product safety and compliance;
    - transport safety;
    - protection of the environment;
    - radiation protection and nuclear safety;
    - food and feed safety, animal health and welfare;
    - public health;
    - consumer protection;
    - protection of privacy and personal data, and security of network and information systems.
- Actions or omissions affecting the financial interests of the EU, as contemplated in Article 325 TFEU, including

conduct undermining EU funds, resources, or financial integrity can also be reported.

- Actions or omissions that impact the internal market within the meaning of Article 26(2) TFEU can also be reported. This includes:
    - breaches of EU rules on competition;
    - breaches of EU rules on State aid; and
    - breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.
- Actions or omissions that may constitute a serious or very serious criminal or administrative offence. In any case, all serious or very serious criminal or administrative offences that involve economic damage to the Public Treasury and Social Security are included.
- Reports concerning labor-law infringements in occupational health and safety are covered, without prejudice to the specific protections provided by the applicable frameworks.
- In addition, the Internal Information System will handle reports concerning violations of ADM's Code of Conduct or any other policy developed in accordance with the Compliance Management System implemented within the Company.

4. Excluded matters and inadmissibility

In accordance with applicable Spanish legislation, this Policy shall not apply to any facts, information, or documents, regardless of their form or medium, that are classified or whose disclosure is restricted for reasons of national security.

Likewise, this Policy shall not apply to information subject to medical or legal professional privilege, to the duty of confidentiality of law enforcement authorities in the exercise of their functions, or to the confidentiality of judicial deliberations and judicial investigations or proceedings.

Furthermore, this Policy shall not apply to information relating to breaches in the conduct of procurement procedures where such information is classified, has been declared secret or confidential, requires the application of special security measures under applicable law, or where the protection of essential State security interests is required.

5. Personal scope

This policy applies to individuals who work in the private or public sector and who have obtained information about reportable breaches in a work-related or professional context, including:

- public sector employees or employees in the private sector;

- self-employed persons;
- shareholders, unit-holders, and members of the administrative, management, or supervisory body of an undertaking, including non-executive members;
- any person working for or under the supervision and direction of contractors, subcontractors, and suppliers.

This policy also applies to reporting persons who communicate or publicly disclose information obtained in the context of:

- an employment or statutory relationship that has ended;
- volunteer activities whether remunerated or not;
- traineeships or internships, whether remunerated or not; and
- recruitment or pre-contractual negotiations, where the information was obtained during the selection process or before the relationship begins.

Where applicable, the protection measures available under this policy extend beyond the reporting person to the following categories, insofar as they may be exposed to retaliation linked to a report or public disclosure:

- workers' legal representatives, when acting in their advisory and support functions to the reporting person;
- individuals who assist the reporting person during the reporting process within the organisation in which the reporting person provides services;
- individuals connected to the reporting person who may suffer retaliation, including co-workers and family members; and
- legal persons for which the reporting person works, or with which the reporting person maintains any other type of relationship in a work-related context, or in which the reporting person holds a significant participation. For these purposes, a participation shall be considered significant where, by virtue of its proportion, it enables the holder to exercise influence over the legal person in which the participation is held, in particular through share capital or voting rights.

For a person to fall within the personal scope of this policy, the information must have been obtained in a work-related or professional context, including current, past, or prospective relationships, and regardless of whether the person reports through internal channels, external channels, or by public disclosure, where legally applicable.

6. Reporting channels and format

Communications or complaints may be made in writing or verbally. The Whistleblowing Channel will be accessible through:

- The whistleblowing website: EthicsPoint - Archer Daniels Midland Company
- telephone numbers: 900 876 240

- by sending an email to the email addresses : canaldenuncias@adm.com

Reports may also request a physical meeting. If a reporter request a physical meeting, this will be set up within a maximum period of seven days.

Verbal communications, including those made through face-to-face meetings shall be documented in one of the following ways, subject to the Reporter's consent:

- by means of a recording of the conversation; or
- by a complete and accurate transcription of the conversation

The Reporter can verify, rectify and agree to the transcription of the conversation by signing it.

The transcripts and minutes may only be kept for the time strictly necessary and proportionate to the processing of the report and to the protection of the Reporters, the persons they refer to and the third parties they mention, as well as to preserve the Company's defense right, taking into account the time required for any further investigations.

Whistleblowers who wish to remain anonymous may do so. In such cases, anonymous communications or complaints received will be handled in accordance with the safeguards established in this Policy and other applicable regulations.

7. Handling standards and timelines

7.1 Receipt and acknowledgement

Where the reporting person has provided contact details (or an anonymous mailbox within the System), acknowledgement of receipt will be issued within seven days, unless doing so would jeopardize confidentiality or the integrity of the process.

7.2 Initial assessment and admissibility

The System Responsible will perform an initial assessment to:

- confirm connection to ADM Group Entities activities;
- confirm material scope;
- assess whether immediate protective measures are needed;
- decide admissibility and the appropriate handling route (internal investigation, referral to a competent internal function, or escalation where legally required).

7.3 Investigation and procedural guarantees

Investigations shall be handled in accordance with applicable law and shall ensure:

- the independence and autonomy of the Responsible Person for the Internal Information System, who shall oversee the handling and investigation of reports;
- the diligent handling of reports and compliance with the applicable time limits by those responsible for managing and investigating reports;
- the confidentiality of the identity of the reporting person, any third parties mentioned, and all actions taken in the handling and processing of the report, ensured by all persons involved in the process;
- the protection of personal data, with access restricted to authorised persons involved in the management, investigation, or support functions of the process;
- respect for the presumption of innocence and the right to honour of the persons concerned throughout the process;
- the right of the affected person to be informed of the acts or omissions attributed to them and to be heard at an appropriate stage, in a manner that ensures the proper conduct of the investigation;
- the referral of information to competent authorities, where required, by the Responsible Person or other authorised functions.

Access to information contained in the Internal Information System shall be limited to authorised persons strictly on a need-to-know basis.

7.4 Feedback and closure of the case

The reporting person shall be informed of the outcome of the investigation within the maximum time limit required by law:

- Three months from acknowledgement of receipt (or, if no acknowledgement was sent, three months from the expiry of the period of seven days after the communication was made).
- This may be extended to a total of six months in duly justified cases due to complexity.

7.5 Referrals to authorities

Confidentiality does not prevent lawful disclosure to competent administrative/judicial authorities when required, and ADM will comply with binding legal obligations to cooperate with authorities.

8. Governance and Internal Information System responsibility

8.1 Oversight

The governing body of ADM Group Entities holds overall responsibility for ensuring the System exists and functions effectively, and for approving this Policy and any material updates.

8.1.1 Internal information System Manager

The management bodies of the entities part of ADM Group in Spain will appoint a natural person who will act as the Internal Information System Manager (the "System Manager") and for approving their dismissal or removal from office. Where the management bodies of the entities part of ADM Group in Spain decides that the System Manager function will be performed by a collegiate body, that body shall delegate to one of its members the day-to-day powers to manage the internal information system and to handle investigation case files, so that there is always a clearly identified individual with operative responsibility for intake, processing and procedural handling of reports.

Both the appointment and any dismissal/removal of (i) the individually appointed System Manager or (ii) the members of the collegiate body (and, where applicable, the member to whom operative powers are delegated) will be notified within ten working days to the Independent Whistleblower Protection Authority (Autoridad Independiente de Protección del Informante) or, where applicable, the competent authority/body of the relevant Autonomous Community, within the scope of its powers. Where the System Manager is dismissed or removed, ADM will ensure that the notification includes the reasons justifying that decision.

The System Manager shall perform their functions independently and autonomously. The System Manager shall not receive instructions of any kind regarding the exercise of their responsibilities under the Internal Information System (including the handling of specific reports, decisions on procedural steps, or the conduct of investigations), and will be provided with the personal and material resources necessary to perform the role effectively.

8.2 Group coordination

The exchange of information between the different companies of the ADM Group will be admissible for the proper coordination and the better performance of their functions.

For the entities belonging to the ADM Group in Spain, the System Manager may implement coordination mechanisms to ensure consistent operation, while ensuring that:

- confidentiality and access restrictions are preserved;
- data transfers are lawful and limited to what is necessary; and
- each entity's legal obligations and governance requirements are satisfied.

9. Confidentiality, records, and data protection

9.1 Confidentiality and restricted access

The Whistleblowing Channel is designed and managed to guarantee the confidentiality of the identity of the whistleblower and any third party mentioned in the complaint and of the actions that are carried out in the management and processing of this, as well as the protection of personal data, preventing access to the corresponding information to unauthorized personnel.

The System is designed to protect:

- the identity of the reporting person (including anonymity where used);
- the identity of affected persons and third parties mentioned; and
- the confidentiality of the report and investigative actions.

Access is limited to authorized persons strictly involved in receipt, assessment, investigation, and resolution.

The Internal Information System has been designed to allow informants who wish to remain anonymous to do so with sufficient guarantees. Therefore, if an informant freely chooses not to conceal their identity, the report resolving the complaint will endeavor not to refer to the informant's identity or that of the parties involved, in order to ensure due confidentiality.

The identity of the person who reports a possible irregularity through the Reporting Channel, if they identify themselves, will be considered confidential information and, therefore, will not be communicated to the person affected by the report or information or to any other third party without their consent.

Notwithstanding the foregoing, data may be provided to both administrative and judicial authorities, to the extent that they are required by such authorities as a result of any procedure derived from the subject of the complaint or information, as well as to the persons involved in any subsequent investigation or legal proceedings initiated as a result of the investigation. Such transfer of data to administrative or judicial authorities will always be carried out in full compliance with legislation on the protection of personal data.

9.2 Data retention

Personal data collected through the Internal Information System will be retained only for the period that is necessary and proportionate to manage the report. In particular, it may be retained: (i) for the time needed to assess whether an investigation should be opened; (ii) where an investigation is opened, for the duration of the investigation and any follow-up measures; and (iii) where applicable, for as long as necessary to exercise or defend legal claims or to comply with legal obligations arising from the matter.

In any event, if no investigation actions are initiated, the information and personal data relating to the report will be deleted no later than three (3) months from receipt. The only exception is where retention is strictly necessary to demonstrate and evidence the proper functioning of the Internal Information System; in that case, the report will be kept only in anonymised form, so that no individuals can be identified.

Lastly and after all of the above, the data collected shall be kept (i) to fulfil any possible legal obligations that may apply; and (ii) to deal with any possible claims and liabilities, keeping such data duly blocked for the maximum legally established periods and at the disposal of the State's security forces, the courts and tribunals and any possible competent public administrations for a maximum legal period of ten years.

9.3 Data protection compliance

Processing of personal data under this Policy will comply with applicable data protection laws (including EU Regulation 679/2016 ("GDPR") and Spanish data protection rules). Key principles applied include:

- purpose limitation (handling and follow-up of reports);
- data minimisation (no unnecessary personal data);
- access control and security;
- restricted disclosure;
- retention limitation; and
- protection of rights of data subjects, managed in a manner that does not compromise confidentiality obligations and the integrity of investigations.

ADM shall not transfer any data it receives through the Whistleblowing Channel to any third parties. Access to such data shall be restricted to personnel who have been duly authorized beforehand by virtue of their functions, responsibilities and duties. Said data may only be provided to third parties to whom ADM is legally obliged to do so, such as, for instance, the courts and tribunals, the State's security forces or any other competent public body.

10. Protection against retaliation and support measures

ADM prohibits any direct or indirect retaliation, threats, and attempts of retaliation against reporting persons and other protected persons identified in Section 5, where the conditions for protection are met.

Retaliation includes any act or omission prohibited by law, or any direct or indirect conduct that causes or may cause unjustified harm or places a person at a disadvantage in the work-related or professional context because of reporting, using external channels, or making a protected public disclosure.

ADM will adopt reasonable measures to prevent, detect, stop, and remedy retaliation, including internal protective steps proportionate to the risk and consistent with applicable law, without prejudice to the legal obligations and the protection of the rights corresponding to natural or legal persons against whom a false Complaint or Information is presented or the Complainant has acted in bad faith.

11. External reporting channels and public disclosure

The reporting person may report their concerns through external reporting channels, in accordance with applicable law, including the Independent Authority for the Protection of Informants or, where applicable, the corresponding regional authorities.

Any natural person may also report to that Authority any breach or omission of the principles and safeguards set out in this document, within the framework of the applicable legal provisions.

The reporting person may also contact other competent authorities to seek advice, support, or to submit their report, benefiting from the protections provided under applicable law.

For information purposes only, some additional external channels at national and European Union level include:

- **European Union – OLAF (European Anti-Fraud Office):** https://anti-fraud.ec.europa.eu/index_en
- **National Anti-Fraud Coordination Service (Spain):** consultasantifraude@igae.hacienda.gob.es

The above list is not exhaustive, and other external channels made available by competent authorities may also be used.

12. Publication and accessibility

This Policy is made available to employees and relevant third parties through appropriate internal and external means, in a manner that is clear, accessible, and easy to locate.

This Policy is reviewed periodically and updated when necessary due to changes in law, regulatory expectations, organizational structure, risks, or operational experience.

This Policy enters into force on the date of approval by the governing body of the entities forming part of the ADM Group in Spain.